UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

924 EAST MAIN STREET, TROY, OHIO, 45373
(including all outbuildings, curtilage, and vehicles parked on the premises)

Case No. 3:21-MJ-51

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A-1

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized):*

SEE ATTACHMENT B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
SEE ATTACHMENT C-1	

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig

Applicant's signature

Andrea R. Kinzig, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ *(specify reliable electronic means).*

Date: 2-8-21

Judge's signature

City and state: Columbus, OH

Chelsey M. Vascura, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO

ATTACHMENT A-1

DESCRIPTION OF LOCATION TO BE SEARCHED

924 EAST MAIN STREET, TROY, OHIO, 45373 ("SUBJECT PREMISES"), is a two-story, single-family residence with white siding. There is a front porch with white pillars leading to the front door. The street address numbers are affixed to the siding next to the front porch. There is a detached one-car garage with white siding and a white overhead door. The SUBJECT PREMISES is located on the north side of East Main Street between East Franklin Street and Williams Street. The SUBJECT PREMISES includes all outbuildings, curtilage, and vehicles parked on the property of the SUBJECT PREMISES.

The warrant authorizes law enforcement officers to remain at the SUBJECT PREMISES during the overnight hours if the search (to include the imaging of any Computer and Electronic Media) cannot be completed prior to 10:00 p.m.

ATTACHMENT B-1

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography), 18 U.S.C. § 922(g) (possession of a firearm by a prohibited person), 21 U.S.C. § 844 (possession of controlled substances), and 21 U.S.C. § 844 (distribution or possession with intent to distribute controlled substances), including but not limited to the following:

Computers and Electronic Media

1. The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with the affidavit submitted in support of this warrant.

2. Computer hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks); cellular telephones and tablets; and digital cameras and recording devices.

3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents, and materials referencing or relating to the above-described offenses. Such records, documents, or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data obtained through computer or Internet-based communications, including data in the form of electronic records, documents, and materials, including those used to facilitate interstate communications, including but not limited to telephone (including mobile telephone), tablets, and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer- related equipment, such as fixed disks, external

hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records and Physical Records

9. Any records related to the possession, receipt, and distribution of child pornography.

10. Any images or videos depicting child pornography.

11. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

12. Any Internet history indicative of searching for child pornography.

13. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.

14. Any communications with minors.

15. Evidence of utilization of email accounts, messenger applications, social media accounts, online chat programs, and peer-to-peer file sharing programs.

16. Any information related to Internet Protocol (IP) addresses accessed by the computer and electronic media.

17. Any Wi-Fi and GPS data associated with the computer and electronic media.

18. Lists of computer and Internet accounts, including user names and passwords.

19. Any computer passwords and encryption keys.

20. Any information related to the use of aliases.

21. Any records, documents, and billing records pertaining to accounts held with telephone, electronic, and Internet service providers.

22. Any and all diaries, notebooks, notes, and other records reflecting personal contact and any other activities with minors.

23. Any children's clothing, toys, or other belongings.

24. Quantities of controlled substances.

25. Any drug paraphernalia, including but not limited to scales used to weigh the controlled substances, items used to package controlled substances (such as baggies, balloons, and

capsules), items used to consume controlled substances (such as pipes, bongs, needles, mirrors, razor blades, straws, spoons, hypodermic needles, and cigarette papers), and items used to dilute or alter controlled substances (such as baking soda, hydrochloride, mannitol, mannite, dextrose, or lactose).

26. Any communications regarding the purchase or sale of controlled substances.

27. Log books, records, payment receipts, notes, and/or customer lists, ledgers, and other papers or electronic records related to the transportation, ordering, purchasing, processing, and distribution of controlled substances.

28. Papers, tickets, notices, credit card receipts, travel schedules, travel receipts, passports, and/or records or other items related to domestic and foreign travel to obtain and distribute controlled substances and drug proceeds, including but not limited to airline receipts, vehicle rental receipts, credit card receipts, travel schedules, diaries, hotel receipts, truck logs, travel agency vouchers, notes, records of long distance telephone calls, emails, and other correspondence.

29. Address and/or telephone books and papers reflecting names, email and physical addresses, and/or telephone numbers of individuals, partnerships, or corporations involved in drug trafficking.

30. Financial records, financial statements, receipts, statements of accounts and related bank records, drafts, letters of credit, money orders, cashier's checks, passbooks, bank checks, escrow documents, and other items evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, secreting, transferring, concealment, and/or expenditure of money.

31. Any surveillance related equipment and any surveillance footage depicting the SUBJECT PREMISES and/or William Sidney Hitchings V.

32. United States currency, precious metals, coins bullion, jewelry, and financial instruments.

33. Photographs and video recordings of controlled substances and drug paraphernalia.

34. Any firearms and ammunition of which WILLIAM SIDNEY HITCHINGS V may reasonably have access to at the SUBJECT PREMISES.

35. Documents and communications related to the purchase and acquisition of firearms and ammunition;

36. Gun boxes, gun holsters, magazines, and other firearm accessories

37. Any records, documents, and billing records pertaining to accounts held with telephone, electronic, and Internet service providers.

38. Any business records related to the operation of Sweeney Communications, Clear Voice One, East Main Technologies, or any other businesses operating at the SUBJECT PREMISES or by WILLIAM SIDNEY HITCHINGS V.

39. Records of personal and business activities relating to the operation and ownership of the computer and electronic media seized from the SUBJECT PREMISES.

40. Documents and records regarding the ownership and/or possession of the items seized from the SUBJECT PREMISES.

Photographs of Search

41. During the course of the search, photographs of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items seized from the residence.

ATTACHMENT C-1

Code Section	Offense Description
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §922(g)	Possession of a Firearm by a Prohibited Person
21 U.S.C. §844	Possession of Controlled Substances
21 U.S.C. §841	Distribution or Possession with Intent to Distribute Controlled Substances

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.

2. Along with other agents, officers, and investigators of the FBI, I am currently involved in an investigation of child pornography, drug, and firearms offenses committed by **WILLIAM SIDNEY HITCHINGS V**. This Affidavit is submitted in support of Applications under Rule 41 of the Federal Rules of Criminal Procedure for search warrants for the following:

   a. The residential property located at **924 East Main Street, Troy, Ohio, 45373** (hereinafter referred to as the "**SUBJECT PREMISES**" and more fully described in Attachment A-1 hereto);

   b. The person of **WILLIAM SIDNEY HITCHINGS V** (hereinafter referred to as "**HITCHINGS**" and more fully described in Attachment A-2 hereto); and

   c. 2011 Chevrolet Tahoe bearing Ohio license plate JEA3406 (hereinafter referred to as the "**SUBJECT VEHICLE**" and more fully described in Attachment A-3 hereto).

3. This Affidavit is submitted in support of Applications for search warrants for the **SUBJECT PREMISES**, the person of **HITCHINGS**, the **SUBJECT VEHICLE**, and the Computer and Electronic Media (as defined in Attachments B-1 through B-3) located at the **SUBJECT PREMISES**, on the person of **HITCHINGS**, and in the **SUBJECT VEHICLE**. The purpose of the Applications is to search for and seize evidence of violations of the following:

   a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess child pornography;

   b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce;

c. 18 U.S.C. § 922(g), which makes it a crime for a prohibited person to possess a firearm;

d. 21 U.S.C. § 844, which makes it a crime to possess controlled substances; and

e. 21 U.S.C. § 841, which makes it a crime to distribute or possess with the intent to distribute controlled substances.

4. The items to be searched for and seized are described more particularly in Attachments B-1 through B-3 hereto and are incorporated by reference.

5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the **SUBJECT PREMISES**, the person of **HITCHINGS**, the **SUBJECT VEHICLE**, and the Computer and Electronic Media (as defined in Attachments B-1 through B-3) located at the **SUBJECT PREMISES**, on the person of **HITCHINGS**, and in the **SUBJECT VEHICLE**.

7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(1), 18 U.S.C. §§ 2252(a)(2) and (b)(1), 18 U.S.C. §§ 2252A(a)(2) and (b)(1), 18 U.S.C. § 922(g), 21 U.S.C. § U.S.C. § 844, and 21 U.S.C. § 841, are present at the **SUBJECT PREMISES**, on the person of **HITCHINGS**, in the **SUBJECT VEHICLE**, and on the Computer and Electronic Media (as defined in Attachments B-1 through B-3) located at the **SUBJECT PREMISES**, on the person of **HITCHINGS**, and in the **SUBJECT VEHICLE**.

PERTINENT FEDERAL CRIMINAL STATUTES

8. 18 U.S.C. § 2252(a)(2) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such

visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

9. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

10. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

11. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

12. 18 U.S.C. §§ 922(g)(1) and (g)(3) states that it is a violation for any person who has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year, or who is an unlawful user of or addicted to any controlled substances, to ship or transport in interstate or foreign commerce, or to possess in or affecting commerce, any firearm or ammunition; or to receive any firearm or ammunition which has been shipped or transported in interstate or foreign commerce.

13. 21 U.S.C. § 844 states that it is a violation for any person to knowingly or intentionally possess a controlled substance unless such substance was obtained directly, or pursuant to a valid prescription or order, from a practitioner, while acting in the course of his professional practice, or except as otherwise authorized by this subchapter or subchapter II of this chapter.

14. 21 U.S.C. § 841 states that it is a violation for any person to knowingly or intentionally (1) manufacture, distribute, or dispense, or possess with the intent to manufacture, distribute, or dispense, a controlled substance, or (2) create, distribute, or dispense, or possess with the intent to distribute or dispense, a counterfeit substance.

BACKGROUND INFORMATION

Definitions

15. The following definitions apply to this Affidavit and Attachments B-1 through B-3 to this Affidavit:

a. **"Child Pornography"** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. **"Visual depictions"** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. **"Minor"** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. **"Sexually explicit conduct"** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

e. **"Internet Service Providers"** or **"ISPs"** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the

subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

f. An **"Internet Protocol address"**, also referred to as an **"IP address"**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

g. **"Hyperlink"** (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

h. **"Website"** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

i. **"Social Media"** is a term to refer to websites and other Internet-based applications that are designed to allow people to share content quickly, efficiently, and on a real-time basis. Many social media applications allow users to create account profiles that display users' account names and other personal information, as well as to exchange messages with others. Numerous forms of social media are presently available on the Internet.

j. **"Exchangeable image file format"**, also referred to as **"EXIF data"**, is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners, and other systems handling image and sound files stored by digital cameras. Most new digital cameras use the EXIF annotation, storing information on images such as shutter speed, exposure compensation, F number, metering system used, if a flash was used, ISO number, date and time the image was taken, etc.

k. **"Metadata"** is data that provides information about other data. For computer files, metadata can be stored within the file itself or elsewhere. Metadata for computer files includes the file name, the file type, where it is stored (*i.e.*, the file path), when it was created, when it was last modified and accessed, the file size, and other information.

l. **"Uniform Resource Locator"** or **"Universal Resource Locator"** or **"URL"** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

m. The terms **"records," "documents,"** and **"materials,"** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Background on Computers and Child Pornography

16. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

17. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a

digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

18. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

19. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

20. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

21. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

22. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's

favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Background on Computer Encryption

23. Encryption is the process of taking plain text and scrambling it into an unreadable format called "cipher text". This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the Internet. When the intended recipient accesses the message, the information is translated back to its original form. This is called decryption. To unlock the message, both the sender and recipient have to use a "secret" encryption key – a collection of algorithms that scramble and unscramble data back to its readable format.

24. Various encryption software is currently available that can encrypt individual files, folders, volumes, or entire disks within a computer, as well as USB flash drives and files stored in the cloud. Examples of some types of encryption software includes BitLocker, AxCrypt, Kruptos 2, and many others. There are two main methods of encryption: symmetric encryption, which involves securing data with a single private key; and asymmetric encryption, which uses a combination of multiple keys that are both public and private.

25. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize encryption on their Computer and Electronic Media to protect their child pornography files from being discovered by their associates and law enforcement officers. When encryption is utilized by the subjects, law enforcement officers typically cannot access the encrypted containers without gaining access to the passwords.

Collectors of Child Pornography

26. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):

a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or

drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

d. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

NCMEC and Cyber Tipline Reports

27. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and

services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.

28. As part of its functions, NCMEC administers the Cyber Tipline. The Cyber Tipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the Cyber Tipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities. Many states utilize Internet Crimes Against Children (ICAC) task forces to serve as the intake organizations for the Cyber Tipline reports. These ICAC's review the Cyber Tipline reports received from NCMEC and assign them to the applicable law enforcement agencies. In Ohio, the ICAC in Cuyahoga County serves as this intake organization.

Cloud Storage

29. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations.

30. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:

a. "Cloud" is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. "The cloud" was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.

b. "Cloud computing" is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

c. "Cloud Service Provider" (CSP) is the entity that offers cloud computing services. CSP's offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage. CSP's maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP's reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long- term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as "electronic storage," and the provider of such a service is an "electronic communications service" provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a "remote computing service." CSP's may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.

d. "Virtual Machine" (VM) is a system where the hardware is virtual rather than physical. Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a VM, does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.

e. "NetFlow Records" are collections of network statistics collected by a service provider about traffic flows. A traffic flow is a sequence of data packets from a source to a destination. NetFlow is collected when it is impractical to collect all of the data packets for a flow. Providers may use these logs for quality control, security, or billing. For any particular network flow, NetFlow can include the source and destination IP addresses, network ports, timestamps, and amount of traffic transferred. A provider may only collect a sample of all possible sessions, and may only store the NetFlow for a short time.

31. Dropbox is an on-line service that allows its users to store files on Dropbox Inc.'s servers. The service is offered by Dropbox Inc., a company based in San Francisco, California.

32. Mega is a cloud storage and file hosting service offered by Mega Limited, an Auckland, New Zealand-based company. Mega is known for its security feature where all files are

end-to-end encrypted locally before they are uploaded. This encryption prevents anyone from accessing the files without knowledge of the pass key.

33. Mega provides its users with the ability to share files or folders with others. One means of sharing files or folders is by creating a "sharing link". A sharing link creates a URL to store the file(s) or folder(s) so that others can access, view, and/or download them. These sharing links can be sent to others via email, Facebook, Twitter, instant message, or other means. Users can limit who can access their sharing links by setting passwords and/or expiration dates for the links.

34. Based on my training and experience, I know that individuals involved in child pornography offenses frequently store their child pornography files in cloud storage accounts such as Mega and Dropbox. I also know, based on my training and experience, that individuals often trade child pornography files by sending sharing links to their cloud storage accounts.

Verizon Location Records and Cloud Data

35. Verizon provides cellular telephone access to the general public. Based on my training and experience, I know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

36. Verizon allows customers to back up and store the contents of their cellular telephones and tablets to a Verizon Cloud. Contents that can be backed up to the Verizon Cloud include messages, images, videos, documents, contacts, and call logs. The Verizon Cloud allows users to wirelessly back up and synch contents between their cellular telephones, tablets, computers, and other devices.

37. Synchronoss Technologies Inc. is a software services company that provides digital, cloud, messaging, and Internet of Things (IoT) platforms to various companies. Verizon has a contract with Synchronoss Technologies Inc. to power, administer, and maintain the Verizon Cloud. Synchronoss Technologies maintains the contents of the cloud accounts associated with Verizon's telephone accounts. However, Verizon maintains the subscriber information, transactional records, and location information for the accounts.

Other Social Media Applications

38. Facebook Inc. is a company based in Menlo Park, California. Facebook Inc. owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

39. Skype owns and operates a communication service that transmits voice calls, video, and messages over the Internet. In May 2011, Skype was acquired by Microsoft Corporation, a company based in Redmond, Washington.

40. Skype users can make and receive local, long distance, and international phone calls; participate in video chats or send and receive video messages; send and receive short message system (SMS) text messages; and send and receive electronic files including documents, pictures, audio, and video.

41. Skype has a feature that provides its users with the ability to exchange Private Conversations. This Private Conversations feature allows users to have end-to-end encrypted audio calls and to exchange end-to-end encrypted text messages, images, videos, and audio files. The contents of these conversations are hidden in the chat notifications in order to keep the information that users share private.

42. Telegram Messenger is a cloud-based instant messaging and voice over IP service that was developed by Telegram Messenger LLP, a privately-held company registered in London, United Kingdom. The application can be downloaded and used free of charge on smartphones, tablets, and computers.

43. Telegram Messenger allows users to exchange messages, photographs, videos, and files of any type. Users can also create groups for up to 200,000 people or channels for broadcasting to unlimited audiences. In addition, Telegram allows users to make voice calls to other users.

44. Kik is a cross-platform instant messenger application available on smartphones. The application is administered by Kik Interactive Inc., a company based in Ontario, Canada. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content. Each Kik user has an account name, which is unique to that user, as well as a profile name.

45. Wickr is an instant messenger application administered by Wickr Inc., a company based in San Francisco, California. The application allows users to exchange end-to-end encrypted and content-expiring messages, photographs, videos, and other file attachments.

46. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize various social media and messenger applications to trade child pornography files and to communicate with other offenders and victims.

FACTS SUPPORTING PROBABLE CAUSE

HITCHINGS' Criminal History

47. Records from the Wilton Manors, Florida Police Department identified that on or around February 25, 2010, officers were dispatched to a motor vehicle crash involving two vehicles. **HITCHINGS** was identified as the driver of the vehicle that caused the crash, and he was cited for making an improper right turn and not having proof of insurance. During a search of **HITCHINGS'** vehicle, officers located the following: (1) two baggies of a white crystalline substance that field tested positive for cocaine; (2) two pill bottles with **HITCHINGS'** name on them that contained suspected Oxycodone and Alpazolam (also known as Xanax); (3) an after-market pill container that contained what appeared to be half of one Alprazolam and approximately five Oxycodone, (4) a white plastic straw and a rolled up dollar bill (two common items of used to consume cocaine); (5) a semi-automatic handgun containing a magazine with nine rounds of 9-millimeter ammunition; and (6) a baggie containing additional 10 rounds of live ammunition. The handgun, cocaine, and pill bottles were located in the same bag. **HITCHINGS** was arrested for Felony Possession of Cocaine, Misdemanor Possession of Drug Paraphernalia, and Felony Possession of a Firearm in the Commission of a Felony.

48. Records from the Broward County, Florida Clerk of Courts identified that on or around November 29, 2020, **HITCHINGS** pled guilty to one count of Felony Possession of Cocaine, in violation of Florida Statute 893.03(2)(a)(4) (a crime punishable by a term of imprisonment exceeding one year). **HITCHINGS** was sentenced to three days of imprisonment. Based on this conviction, **HITCHINGS** is prohibited from possessing firearms.

Information from Cooperating Witness

49. Beginning in or around December 2019, I have been involved in an investigation of child pornography offenses committed by an adult male who will be referred to for purposes of this Affidavit as "Adult Male A". Adult Male A has pled guilty in the United States District Court for the Southern District of Ohio to one count of production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and (e). As part of his plea agreement, Adult Male A admitted that he had produced child pornography in 2019 and that he had viewed child pornography files depicting other children.

50. As part of the investigation, Adult Male A was interviewed on two occasions in March 2020 and May 2020. During these interviews, Adult Male A identified that he had received child pornography files from an individual who lived in Troy, Ohio. During the first interview, Adult Male A referred to this individual as "WILLIAM" and advised that WILLIAM's last name might be **HITCHINGS** or HIGGINS. During the second interview, Adult Male A advised that this individual's name was either "WILL HIGGINS" or "WILL **HITCHINGS**".

a. I know, based on my training and experience, that WILL is a common nickname for WILLIAM. It is common, in my experience, for individuals to transpose nicknames with true names.

b. Based on the information Adult Male A provided about the individual who sent him the child pornography, there is probable cause to believe that Adult Male A was referring to **HITCHINGS**.

51. During the first interview in March 2020, Adult Male A minimized his involvement in child pornography activities. He only admitted that he received and viewed child pornography on a limited number of occasions, and he denied that he produced child pornography. Below is a summary of information that Adult Male A provided about **HITCHINGS** during the first interview:

a. Adult Male A reported that he received at least one video depicting child pornography from **HITCHINGS** on a past occasion. **HITCHINGS** sent this video to Adult Male A via Telegram. Adult Male A acknowledged that there may have been additional occasions in which **HITCHINGS** sent him (Adult Male A) child pornography files.

b. Adult Male A stated that he did not want to get **HITCHINGS** in trouble, but that **HITCHINGS** was "into" child pornography.

c. Adult Male A had been to **HITCHINGS'** residence in the past. Adult Male A saw **HITCHINGS** view child pornography and bestiality files on a computer that was in **HITCHINGS'** residence.

d. **HITCHINGS** had a large rack of computers inside of his residence.

e. Adult Male A described **HITCHINGS'** residence as being on State Route 41 (also known as Main Street) near a school in Troy, Ohio.

52. Adult Male A was interviewed again in May 2020 pursuant to his arrest. During this interview, Adult Male A admitted that he had produced, received, and distributed child pornography files. He also provided additional information about **HITCHINGS** during this

interview. Below is a summary of information that Adult Male A provided about **HITCHINGS** during the second interview:

a. On the first occasion that Adult Male A was at **HITCHINGS'** residence, **HITCHINGS** took Adult Male A into the basement. **HITCHINGS** had a black rack of computers in the basement. **HITCHINGS** asked if Adult Male A wanted to see some "crazy" videos and then proceeded to show Adult Male A videos depicting bestiality and child pornography.

b. Over one year ago, **HITCHINGS** gave Adult Male A a desktop computer that was "packed" full of child pornography and adult pornography files. The pornography included children having sex with other children and animals. Adult Male A later destroyed the hard drive that was in this desktop computer.

c. **HITCHINGS** also at one time gave Adult Male A a laptop computer that contained child pornography files.

d. **HITCHINGS** previously told Adult Male A that there was good child pornography on Telegram.

e. Adult Male A again described **HITCHINGS'** residence as being on State Route 41 near a school and where the road curved. Adult Male A identified that **HITCHINGS** lived with his boyfriend, CHRIS (no last name provided), and **HITCHINGS'** mother.

53. It was noted that during both of the interviews of Adult Male A, he sometimes talked about how his deceased relatives and God spoke to him. However, Adult Male A provided information about his child pornography activities that was consistent with other information obtained pursuant to the investigation, including information provided by victims and cooperating witnesses, information obtained from Adult Male A's electronic accounts pursuant to search warrants, and other information obtained pursuant to the investigation. It is therefore reasonable to believe that the information Adult Male A provided about **HITCHINGS** is credible.

54. It was also noted that Adult Male A provided more information about his own child pornography activities as well as **HITCHINGS'** child pornography activities during the second interview (which was conducted pursuant to Adult Male A's arrest). Based on my training and experience, I know that it common for individuals to withhold information about their criminal activities when first contacted by law enforcement officers. Individuals often withhold such information as a means to protect themselves and their co-conspirators from criminal culpability. It is not uncommon for such individuals to be more truthful

during subsequent interviews when they are faced with additional evidence and/or during interviews conducted after they have been arrested.

Cyber Tipline Report

55. As part of the investigation, I have learned that Synchronoss Technologies Inc. filed a report to NCMEC's Cyber Tipline on or around November 23, 2020, regarding approximately six suspected child pornography or child exploitation files located in a Verizon Cloud account associated with telephone number 937-554-7700 (hereinafter referred to as the "TARGET CELL PHONE"). Synchronoss Technologies Inc. provided these approximately six suspected child pornography or child exploitation files to NCMEC as part of its Cyber Tipline report.

56. NCMEC forwarded Synchronoss Technologies Inc.'s Cyber Tipline report, along with the suspected child pornography or child exploitation files, to me for further investigation. Based on my review of the files and my training and experience, I believe that approximately six of the files depict child pornography. By way of example, three of the files are described as follows:

a. a968ea8e58fa4b458ed2f98b600f626f_file1.jpg: The file is an image that depicts what appears to be a nude pre-pubescent white male child who is lying on his back with his legs spread apart, exposing his nude genitals to the camera. What appears to be an adult white male (whose face is not captured in the image) appears to be urinating on the child.

b. a968ea8e58fa4b458ed2f98b600f626f_file2.jpg: The file in an image that depicts what appears to be a nude pre-pubescent white male child performing fellatio on what appears to be an adult white male (whose face is not captured in the image).

c. a968ea8e58fa4b458ed2f98b600f626f_file3.jpg: The file is an image that depicts what appears to be two nude pre-pubescent white male children who are standing next to each other. One child is touching the other child's penis.

Records Obtained Pursuant to Search Warrants and Subpoenas

57. On or around January 12, 2021, Synchronoss Technologies Inc. was served with a search warrant requesting the account contents of the Verizon Cloud account associated with the TARGET CELL PHONE (hereinafter referred to as the "SUBJECT VERIZON CLOUD ACCOUNT"). The account contents provided by Synchronoss Technologies Inc. in response to the search warrant included approximately seven documents, approximately 1,647 image files, and approximately 90 video files. Below is a summary of information noted regarding these files:

a. More than 450 of the image and video files depicted a male who appears to be **HITCHINGS**. The following was noted regarding these files:

i. The EXIF data and metadata for the images and videos indicated that they were produced during the approximate time period of 2013 through 2020.

ii. The EXIF data indicated that the following devices were utilized to produce the images: a Motorola Moto z3 (the device associated with the TARGET CELL PHONE), a GoPro Hero 4, an LGE Nexus 4 cellular telephone, an LG Model LG-H918 cellular telephone, a Kyocera Model E6830 cellular telephone, and approximately nine different models of Samsung cellular telephones.

iii. A number of the images and videos depicted **HITCHINGS** engaged in sexually explicit conduct. Some of the images and videos depicted **HITCHINGS** engaged in sexually explicit conduct with a dog.

iv. A number of the images and videos depicted **HITCHINGS** in what appears to be a basement. Numerous computer and electronic media (including computers, computer servers, computer hardware, and suspected surveillance systems) were depicted in the images and videos of **HITCHINGS**. **HITCHINGS** was depicted accessing these computer devices in some of the images and videos.

1. As noted above, Adult Male A reported that **HITCHINGS** had a large rack of computers in his basement.

v. Approximately 15 of the images depicted **HITCHINGS** standing in what appears to be a kitchen. In approximately seven of the 15 images, it appears that **HITCHINGS** was wearing a holster on his pants with a handgun inside the holster. In approximately eight of the 15 images, **HITCHINGS** was holding the handgun and/or putting the handgun down his pants. The EXIF data associated with these approximately 15 images indicates that they were produced on or around July 16, 2016.

vi. One image depicted **HITCHINGS'** Ohio driver's license.

b. Approximately 28 of the images depicted what appears to be a Sports Utility Vehicle. The EXIF data for these images identified that they were produced on or around September 6, 2020 and September 24, 2020. **HITCHINGS** was depicted sitting in the driver's seat of the vehicle in approximately two of the images. The

license plate was depicted in approximately three of the images, and the license plate matched that of the **SUBJECT VEHICLE.**

c. One image depicted a screen print of what appears to be an order confirmation from an Internet-based purchase, with **HITCHINGS'** name and the **SUBJECT PREMISES** listed as the apparent purchaser.

d. Approximately three images depicted three packages from the United States Postal Service and United Parcel Service, all of which were addressed to **HITCHINGS** at the **SUBJECT PREMISES.** Approximately one image depicted a Packing List for an order, with **HITCHINGS'** name and the **SUBJECT PREMISES** listed as the recipient of the items on the document.

e. In addition to the images and videos depicting **HITCHINGS** with computer devices, numerous other images and videos depicted computer and electronic media – including computers, computer servers, computer hardware, and surveillance systems. Some of the images depicted what appears to be monitoring screens for the surveillance cameras. Based on these images as well as other information obtained pursuant to the investigation, it appears that there are surveillance cameras that capture both the interior and exterior of **HITCHINGS'** residence, and that monitoring screens for these cameras are located both in the basement and the living room of the residence.

   i. Based on my training and experience, I know that individuals involved in criminal activities often utilize surveillance cameras as a means to both protect their homes from thefts (such as thefts from other drug suppliers and drug users) and to monitor their homes for any potential contact with law enforcement officers.

f. One image depicted what appears to be a screen print from an Internet website. This screen print listed the email address of w.hitchings@gmail.com.

g. Approximately eight of the images depicted what appears to be child pornography. Six of these files were the same as those reported in the Cyber Tipline report filed by Synchronoss Technologies Inc. (as detailed above). The other two files are described as follows:

   i. Felixxx_134931EdF_koz.jpg: The file is an image that depicts what appears to be a nude toddler-aged male child. The child's legs are straddled, exposing his nude genitals and anus to the camera. It appears that the child's legs are bound to his arms with black tape. What appears to be an adult white male (whose face is not captured in the image) is pointing his penis toward (or possibly touching his penis to) the child's leg and penis.

ii. Felixxx_143309iCO_6598.jpg: The file is an image that depicts what appears to be a pre-pubescent white male child. The child is turned upside down over the lap of what appears to be an adult white male (whose face is not captured in the image). The child's pants are pulled down, exposing his nude genitals and anus to the camera. The adult male's hands are touching the child's legs and buttocks. The adult male's penis is exposed and pointed over the child's buttocks.

h. Approximately two of the images depicted what appears to be nude pre-pubescent male children.

i. At least approximately 22 of the images and videos depicted substances that, based on my training and experience, appear to be controlled substances. These files included the following:

i. Approximately 10 of the images and videos depicted a green leafy substance that appears consistent with marijuana. In one of the images, the substance was contained in a foil pan placed on a scale, with the scale showing a weight of 1.69 ounces. Other images depict the substance contained in large bags or a bowl.

1. Based on my training and experience, the quantities of the suspected marijuana depicted in some of the images are consistent with distribution amounts.

ii. Approximately four of the images and videos depicted a crystal rocky substance that appears consistent with methamphetamine. One of these images depicted the crystal substance in a Tupperware container on a scale, with the scale showing a weight of 26.21 grams.

1. Based on my training and experience, some of the quantities of suspected methamphetamine depicted in the images (including the one showing an approximate weight of 26.21 grams) are consistent with distribution amounts.

iii. Approximately five of the images and videos depicted a white rocky substance that appears consistent with crack cocaine or methamphetamine. Approximately two of the images depicted the substance in bags on a scale, with the scale showing weights of 2.04 grams and 0.79 grams.

iv. Approximately three videos depicted an individual smoking a substance from a bong.

v. The EXIF data for the images identified that they were produced with a Motorola Moto z3 cellular telephone (the device associated with the TARGET CELL PHONE) during the approximate time period of August 1, 2019 through November 1, 2020. The background shown in some of the images and videos appears to match the background of the basement where **HITCHINGS** was captured in other images and videos (as detailed above).

j. One of the documents had a title on the first page of the following: "Dome Network Camera Quick Start Guide". This document provided instructions on how to use a dome surveillance camera. Another document was entitled "Family Fun". This document required a password to access it, and as such, could not be viewed.

i. Based on my training and experience, I know that the need to input a password to access a file is indicative that it is encrypted.

58. Based on the information contained in the SUBJECT VERIZON CLOUD ACCOUNT as well as other information detailed in the Affidavit, it appears that **HITCHINGS** has had access to numerous computer devices. It also appears that **HITCHINGS** has had access to controlled substances.

59. On or around January 12, 2021, Verizon was served with a search warrant requesting information associated with the TARGET CELL PHONE (including historical cell site records) for the time period of January 1, 2020 through January 12, 2021. Records received from Verizon in response to the search warrant included the following information:

a. The TARGET CELL PHONE was subscribed to CHRISTOPHER SWEENEY (hereinafter referred to as "SWEENEY") at the **SUBJECT PREMISES**. The contact person listed for the account was **HITCHINGS**. **HITCHINGS'** address was also listed as being the **SUBJECT PREMISES**.

i. Based on my training and experience, I know that individuals' telephone accounts may be subscribed to in other persons' names for a variety of reasons. One such reason could be that the individual has poor credit. Another reason could be that the person is on a "family plan" with a relative(s) or friend(s). Yet another reason could be to conceal the person's identity when the telephone account is being used in furtherance of illegal activities.

ii. As detailed above, Adult Male A identified that **HITCHINGS** resided with his boyfriend, whose first name was "CHRIS". Based on the investigation

conducted to-date, it appears that SWEENEY and **HITCHINGS** are involved in a romantic relationship.

b. The device that utilized the TARGET CELL PHONE was a Motorola Moto z3 cellular telephone.

c. The historical cell site records for the TARGET CELL PHONE identified that it was consistently in the area of the **SUBJECT PREMISES**, including during overnight hours.

d. The historical cell site records were compared to two of the dates associated with the photographs of marijuana that were recovered from the SUBJECT VERIZON CLOUD ACCOUNT (some of those detailed above in paragraph 57(i)(i)). This comparison provided the following information:

i. The EXIF data for approximately four of the photographs of marijuana recovered from the SUBJECT VERIZON CLOUD ACCOUNT identified that the photographs were produced with a Motorola Moto z3 cellular telephone on or around April 17, 2020 between approximately 8:31 a.m. and 11:46 a.m. One of these images depicted the marijuana on a scale (showing a weight of 1.69 ounces) and three of the images depicted the marijuana in an aluminum container and/or bowl. The cell site records identified that the TARGET CELLL PHONE was in the area of the **SUBJECT PREMISES** before, during, and after this approximate time period.

ii. The EXIF data for approximately three of the photographs of marijuana recovered from the SUBJECT VERIZON CLOUD ACCOUNT identified that the photographs were produced with a Motorola Moto z3 cellular telephone on or around November 1, 2020 at approximately 8:07 p.m. The cell site records identified that the TARGET CELL PHONE was in the area of the **SUBJECT PREMISES** both before and after this approximate time – specifically, that it was in the area of the **SUBJECT PREMISES** at approximately 7:57 p.m. and 8:23 p.m.

iii. Based on the information detailed above, as well as other information associated with the photographs (i.e., the items depicted in the background of the photographs), it is reasonable to believe that the quantities of marijuana from the images detailed above were photographed inside the **SUBJECT PREMISES**.

60. As part of the investigation of Adult Male A, records were obtained from Facebook Inc. pursuant to a search warrant for his Facebook account. These records identified that Adult

Male A had "blocked" another Facebook account containing a profile name of "**WILLIAM HITCHINGS**" and a user identification number of 100003978596185. On or around January 13, 2021, an administrative subpoena was served to Facebook Inc. requesting subscriber information for the Facebook account with the user identification number of 100003978596185, as well as logs of IP addresses utilized to access the account. Records received in response to the subpoena provided the following information:

a. The account was created on or around June 20, 2012 in the name of "**WILLIAM HITCHINGS**". The vanity name for the account was whitchings.

b. The email address associated with the account was hitchingsw@gmail.com. The telephone numbers associated with the account were the TARGET CELL PHONE and telephone number 305-587-8639.

c. The log of IP addresses identified that the two most common IP addresses utilized to access the account were 71.66.197.244 and 71.66.197.242. The account was accessed as recently as on or around January 11, 2021.

61. On or around January 14, 2021, an administrative subpoena was served to Google LLC requesting subscriber information for the w.hitchings@gmail.com Google account (the email address that appeared in one of the images recovered from the SUBJECT VERIZON CLOUD ACCOUNT), as well as logs of IP addresses utilized to access the account. Records received in response to the subpoena provided the following information:

a. The account was created on or around September 12, 2004 in the name of "**WILLIAM HITCHINGS**".

b. The alternate email address listed for the account was wenglebot@yahoo.com. The sign-in telephone number for the account as well as the recovery telephone number for the account were both listed as being the TARGET CELL PHONE.

i. Based on my training and experience, I know that many email providers such as Google LLC ask their users to provide alternate or recovery email addresses and telephone numbers when signing up for email accounts. The email providers send various notifications regarding the use of the users' email accounts to the alternate email addresses and telephone numbers to serve as security measures (i.e., to ensure that users' accounts have not been hacked or otherwise compromised). The email provider may also send to the user's alternate account a verification code that is needed to change a password to the user's account or complete other account maintenance.

c. The log of IP addresses identified that the two most common IP addresses utilized to access the account were 71.66.197.244 and 71.66.197.242 (the same IP addresses

utilized to access the whitchings Facebook account). The account was accessed as recently as on or around January 11, 2021.

62. Charter Communications was identified as the Internet Service Provider for the IP addresses of 71.66.197.244 and 71.66.197.242 (the IP addresses utilized to access the w.hitchings@gmail.com Google account and the whitchings Facebook account). On or around January 19, 2021, an administrative subpoena was served to Charter Communications requesting subscriber information for these IP addresses on a sample of two of the dates and times that they were utilized to access the w.hitchings@gmail.com Google account. Records received from Charter Communications in response to the subpoena identified that they were both subscribed to East Main Technologies Inc. at the **SUBJECT PREMISES**.

63. As part of the investigation, FBI investigators reviewed publicly available information on various social media websites and messenger applications for any possible accounts associated with the TARGET CELL PHONE and the email addresses w.hitchings@gmail.com, hitchingsw@gmail.com, and wenglebot@yahoo.com. Among other accounts, investigators located the following:

a. Google accounts were located that were associated with the email addresses hitchingsw@gmail.com and w.hitchings@gmail.com. The profile pictures for these two accounts depicted a white male who appears to be **HITCHINGS**.

b. A Skype account was located that was associated with the email address w.hitchings@gmail.com. This Skype account contained a user name of "o0bc0o" and a profile name of "WILLIAM".

c. A Dropbox account was located that was associated with the email address w.hitchings@gmail.com.

d. A Telegram account was located that was associated with the TARGET CELL PHONE. The account had a display name of "Bee Cee" and a user name of "o0bc0o" (the same user name as the Skype account listed above). The account was presently offline.

i. As detailed above, Adult Male A identified that he received one or more child pornography files from **HITCHINGS** via Telegram.

64. On or around January 20, 2021, Microsoft Corporation was served with a search warrant requesting information associated with the Skype account with the user name of o0bc0o and/or associated with the email address w.hitchings@gmail.com. Records received from Microsoft Corporation in response to the search warrant included the following information:

a. The account was created on or around June 24, 2015 in the name of **"WILLIAM HITCHINGS"**. The account was associated with the email address w.hitchings@gmail.com.

b. The o0bc0o Skype account user exchanged hundreds of chat messages directly with other users (hereinafter referred to as "User Chats"). These User Chats included the exchange of text messages, image and video files, and live video calls (of which the contents could not be provided by Microsoft Corporation). At least approximately 14 of the image and video files sent by the o0bc0o Skype account user depicted **HITCHINGS**.

c. The User Chats revealed that on or around February 16, 2020, the o0bc0o Skype account user exchanged messages with another user who will be referred to for purposes of this Affidavit as "Skype User-1". The o0bc0o Skype user and Skype User-1 discussed a website that promoted individuals who have a sexual fetish in gear, which they referred to as a gear fetish or "GF". During the exchange, the o0bc0o Skype user sent a picture of a server that was consistent with some of the pictures recovered from the SUBJECT VERIZON CLOUD ACCOUNT. The o0bc0o Skype user made comments indicating that this server had a large storage capacity that could host the gear fetish website. Below are excerpts from this chat:

o0bc0o:	idk if I said before, but I have the means to kickstart a site and host it free and clear of everyone else.
o0bc0o:	idk if gf domain is available, and the variations off gearfetish don't play out so well
o0bc0o:	*Sends image of a computer server*
o0bc0o:	this is growing. storage is now redundant at 100tb
Skype User-1:	Oh really?
o0bc0o:	two cables lines and a metro E leased line. I can literally recreate GF and handle the traffic.

i. Based on my training and experience, I know that 100 terabytes (TB) consists a very large amount of computer data. Hard drives contained in typical laptops and computers are generally 500 gigabytes (GB) to two TB.

d. The User Chats revealed that during the approximate time period of March 16, 2019 through February 2, 2020, the o0bc0o Skype user exchanged messages with another user who will be referred to for purposes of this Affidavit as "Skype User-2". During their communications, they appeared to communicate about child pornography and drug activities. These communications included the following:

i. The o0bc0o Skype user and Skype User-2 made comments indicating that they also communicated with each other via the Telegram, Wickr, and Kik smartphone messenger applications. There were also times when Skype User-2 sent the o0bc0o Skype user sharing links to Mega accounts. Based on the context of the communications, it appeared that the o0bc0o Skype user and Skype User-2 may have also traded child pornography files with each other via Telegram, Wickr, Kik, and/or Mega sharing links. By way of example, on or around January 25, 2020, Skype User-2 sent the o0bc0o Skype user a sharing link to a Mega account. Skype User-2 thereafter stated the following: "Here to keep that cock hard, have you found any groups here wickr or kik try to find more pedos[1]".

ii. During the approximate time period of May 7, 2019 through May 9, 2019, the o0bc0o Skype user made comments indicating that administrators of the Mega cloud storage service had found child pornography files in his Mega account and closed the account. The o0bc0o Skype user talked about his fears that law enforcement officers would execute a search warrant at his residence, and he also expressed thoughts of committing suicide. The o0bc0o Skye user made comments indicating that he possessed and carried a 9-millimeter handgun. The o0bc0o Skype user made other comments indicating that he thought he had taken necessary precautions to prevent his accounts from being detected. The o0bc0o Skype user also made comments about how law enforcement officers would not find anything on his computer media if a search warrant was in fact executed at his residence. Furthermore, the o0bc0o Skype user talked about how law enforcement officers previously executed a search warrant on a prior residence and did not locate any evidence. Based on my training and experience, these comments are consistent with someone who stores child pornography files on a cloud service and/or a server and/or possesses devices that utilize encryption. Below are excerpts from these communications:

o0bc0o:	Mega flagged my account
o0bc0o:	I'm out of this forever my homey.
Skype User-2:	Which one?
o0bc0o:	It doesn't matter.
Skype User-2:	What
Skype User-2:	Don't leave me
Skype User-2:	Lol
Skype User-2:	Will Miss you after all those years
o0bc0o:	check all your shit
o0bc0o:	check it

1 Based on my training and experience, I know that "pedo" is a term to refer to a pedophile or an individual who has a sexual attraction to children.

o0bc0o:	methinks there are those among us…fucking with shit
Skype User-2:	What??
Skype User-2:	Your ok
o0bc0o:	no, I'm not ok
Skype User-2:	What's going on
Skype User-2:	You scare me like this
o0bc0o:	Mega account got flagged
o0bc0o:	gave me a warning by email
o0bc0o:	second email 3 days ago, I just found it.
o0bc0o:	DIDN'T KNOW THEY COULD LOOK AT YOUR ENCRYPTED STORAGE
Skype User-2:	Damn close it and delete
o0bc0o:	generic threat went out. They know who I am.
o0bc0o:	they have DIRECT connection between the account and a paypal!
o0bc0o:	But if they sent out an email saying warning, then…
o0bc0o:	the second email they deleted the account….hold on I'll fucking show you
o0bc0o:	*Sends partial excerpt from an email that appears to be from the Mega website, addressed to aaggll@yahoo.com. Below is an excerpt from this message:*

"Recently you were sent an email advising that your account was found to contain copies of files that were reported to as being objectionable under Section 31(1)(A) of the New Zealand Films, Videos, and Publications Classification Act 1993. In particular, this relates to depictions of sexual conduct with or by children, or young persons (Section 3(3)(a)(iv)), which is an offense carrying potentially lengthy prison sentences in your jurisdiction."

Skype User-2:	Which account was it your cp account?
o0bc0o:	Yes.
o0bc0o:	The email says
o0bc0o:	WE DELETED IT
o0bc0o:	DONT DO IT AGAIN
o0bc0o:	DONT COME BACK TO MEGA
oObc0o:	I paid for premium service, that goes back to my name.
o0bc0o:	Now…would I get a heads up if they were about to raid me?
o0bc0o:	no, of course not.
o0bc0o:	and how expensive would it be to give me a week heads up to dump all physical anythings?
o0bc0o:	and THEN Raid me?

o0bc0o:	very unlikely. I'm not that interesting.
Skype User-2:	Have you deleted your account yet?
o0bc0o:	YUes
Skype User-2:	Fuck
o0bc0o:	but it doesn't mean it's not archived, on ice for someone to look at down the road
o0bc0o:	There's not data on any systems or disk I possess. If they raid me if they fuck with me, it'll be a pain in the ass, but ultimately yield a bunch of shit it would cost a fortune for them to hold me to charge wise.
o0bc0o:	sigh
Skype User-2:	Positive thinking
o0bc0o:	I thought I knew all the ins and outs.
o0bc0o:	I fucking know security
Skype User-2:	You will be fine
o0bc0o:	I don't know where I lapsed.
o0bc0o:	I might not
Skype User 2:	Exactly
Skype User 2:	Exactly
o0bc0o:	You see, this happened before, the attorney general in my parents home state…raided my childhook home
o0bc0o:	did I ever tell you this?
Skype User-2:	No
o0bc0o:	They raided a home that had been vacant for 2 years.
o0bc0o:	they raided looking for a single video download
o0bc0o:	ONE tagged download from emule or some shit.
o0bc0o:	ONE BY FILE NAME
Skype User-2:	When was that
o0bc0o:	years ago. The house was empty.
o0bc0o:	So they went down the street where my family had their new house
o0bc0o:	got a new warrant
Skype User-2:	Did they find you ,?
o0bc0o:	took all their shit. Had to give it back because theyere was nothing to find
	. . . . .
o0bc0o:	even if I turn out safe…and take every precaution…
Skype User-2:	Always
o0bc0o:	how the fuck will I know I can stop looking over my shoulder.
o0bc0o:	I fucking cant
o0bc0o:	I almost shot myself yesterday.
o0bc0o:	I almost blew my brains out
Skype User-2:	With drugs I hope

o0bc0o:	No, with a fucking nine mill[2].
Skype User-2:	Fuck no
o0bc0o:	Oh god I wanted to so bad.
Skype User-2:	Don't do that
o0bc0o:	so much to lose
Skype User-2:	A waist of a nice cock and body lol
o0bc0o:	Could be very real.
o0bc0o:	Not knowing if a bunch of armed men might show up ANY TIME for YEARS to come…
o0bc0o:	I will never sleep again.
o0bc0o:	And I've been carrying my firearm again.
Skype User-2:	Move to another state
o0bc0o:	doesn't work like that
o0bc0o:	They know where I am
	. . . . .
o0bc0o:	cops…federal agents…these people LIVE to kill people like me.
o0bc0o:	and child porn is what ANY good Christian police type will kill over.
	. . . . .
o0bc0o:	Everyone around here gets followed.
o0bc0o:	sometimes stopped, yes.
o0bc0o:	I should just start killing them
o0bc0o:	slam the brakes on and be like OMG OFFICER I DIDN'T SEE YOU THERE
o0bc0o:	a deer came across the road
o0bc0o:	and when he approaches the car
Skype User-2:	Don't do that you will be inside st least lots if boys to fuck
o0bc0o:	shotgun blast the pig in the face.
Skype User-2:	Messy
o0bc0o:	turns me the fuck on
o0bc0o:	I hate them
o0bc0o:	stealing my life.

iii. On or around January 19, 2020, the o0bc0o Skype user talked to Skype User-2 about his apparent sexual interest in the children of a man with whom he had a sexual relationship. These comments included the following:

o0bc0o:	an unexpected surprise. The boy I was fucking I thought gave me HIV, he's sort of here all the time now. Body looks like a cut 16 year old. Had a couple

2 Based on the context of the communications and my training and experience, I believe that the oObc0o Skype user was referring to a 9-millimeter handgun.

	daughters and talks to me about wanting to fuck them, things of that nature. Very bi, very suggestible, does what I tell him to do.
o0bc0o:	Anyway, he's into it, so fresh files, very helpful in encouraging that behavior
	. . . . .
o0bc0o:	he doesn't seem to mind camming. Thought I'd take him into a cam session of pedos and make him represent me
Skype User-2:	Mmmm good fuck toy, you may get him knotted mm
o0bc0o:	I will teach him about k9
o0bc0o:	and if he has any kids, I'm going to get inside of them too.
o0bc0o:	he might be a connection to that world
o0bc0o:	*Emoticon*
Skype User-2:	Make sure you going to film that for me
Skype User-2:	All of it
o0bc0o:	yup

iv. On or around February 2, 2020, the o0bc0o Skype user made comments indicating that he was in possession of controlled substances, and that he shared these controlled substances with his associates. The o0bc0o Skype user also made comments indicating that he had made gummy bears that caused people to become unconscious. Based on my training and experience, I know that individuals involved in drug offenses often lace gummy bears with THC[3]. Furthermore, the o0bc0o Skype user made comments indicating that he had shown child pornography to his "runner"[4]. Below are excerpts from this conversation:

Skype User-2:	What's happening any good porn
o0bc0o:	nah.
o0bc0o:	I got a TINY bit of drugs though.
Skype User-2:	Mmm so you getting high …nice
o0bc0o:	*Sends image of a crystal substance that appears consistent with methamphetamine (and that appears consistent with a distribution amount)*
o0bc0o:	Two ounces
Skype User-2:	Mmm
Skype User-2:	Party time
o0bc0o:	All the time because it pretty much refills itself

3 Tetrahydrocannabinol, or THC, is a psychoactive compound in cannabis that produces a high sensation.

4 Based on my training and experience, I know that individuals involved in drug trafficking offenses use the term "runner" to refer to individuals who transport drugs for them.

o0bc0o:	I also made gummy bears
o0bc0o:	Anyone and everyone who eats one of them unavoidable becomes unconscious for 4 to 6 hours
Skype User-2:	Nice way to rape hehe
o0bc0o:	Like this stuff is stronger than valium or xanax
o0bc0o:	Yah
o0bc0o:	Def for rapes
o0bc0o:	Hehe
Skype User-2:	Nice any coming over
Skype User-2:	Who are the lucky ones to be used hehe
Skype User-2:	Lifeless fuck toy cum dump
o0bc0o:	*Sends video file depicting what appears to be **HITCHINGS** having anal intercourse with another male*
	. . . . .
Skype User-2:	Mmm nice which bitch is that
o0bc0o:	My runner.
o0bc0o:	He gets what I need
Skype User-2:	Your load lol
o0bc0o:	Hah among other things
o0bc0o:	He likes girls and guys.
o0bc0o:	Not so sure about boys
o0bc0o:	But I make him watch it.
Skype User-2:	Mmm horny what you show him
Skype User-2:	Hsrd fucking or just boys playing
o0bc0o:	Toddler. Rapey stuff.
o0bc0o:	Hard fucking or just bored is playing? When do I just watch them play? That's not good enough. I always watch them fuck.

65. On or around January 20, 2021, Dropbox Inc. was served with a search warrant requesting information associated with the Dropbox account associated with the email address w.hitchings@gmail.com. Records received from Dropbox Inc. in response to the search warrant included the following information:

a. The account was created on or around November 10, 2012, in the name of "**WILLIAM HITCHINGS**". The account was associated with the email address w.hitchings@gmail.com.

b. The account was accessed as recently as on or around January 11, 2021, utilizing an IP address of 71.66.197.244 (the same IP address utilized to access the whitchings Facebook account and the w.hitchings@gmail.com Google account, and that is subscribed to East Main Technologies at the **SUBJECT PREMISES**).

c. The contents of the Dropbox account included images and videos depicting computer servers and other computer and electronic media.

d. The contents of the Dropbox account included a text file with a file name starting with "BitLocker Recovery Key" followed by a series of additional characters. This document appears to provide a BitLocker encryption recovery key. The records from Dropbox Inc. identified that this text file was uploaded to the Dropbox account on or around March 4, 2018. Other log files provided by Dropbox Inc. identified that a PDF file with a file name of "new bitlocker key.pdf" was uploaded to the Dropbox account on or around May 11, 2016, but then deleted from the account on the same day.

i. Based on this and other information detailed in the Affidavit, it appears that **HITCHINGS** has utilized encryption on one or more of his computer devices.

e. The contents of the Dropbox account included images and videos depicting **HITCHINGS**. One of the videos displayed multiple still images of **HITCHINGS**. A number of the still images in the video file depicted **HITCHINGS** with what appears to be a handgun on his person, either in a holster on his pants or held in his hands (some of which appeared to be the same as or similar to the images recovered from the SUBJECT VERIZON CLOUD account, as detailed above). The records from Dropbox Inc. identified that this video file was uploaded to the Dropbox account on or around February 5, 2017.

f. The contents of the Dropbox account included an image depicting a quantity of currency spread out on a table or desk. It appears that the currency included over $1,900, including multiple $100 bills. Also depicted on the same table or desk were two cellular telephones, a computer keyboard, **HITCHINGS'** Michigan driver's license, a hatchet, two machetes, and various other items. The records from Dropbox Inc. identified that this image was uploaded to the Dropbox account on or around February 19, 2019.

i. Based on my training and experience, I know that individuals involved in drug trafficking offenses and other criminal activities often photograph the proceeds of their criminal activities.

Other Records

66. Based on review of a police report of the West Milton (Ohio) Police Department, I learned that on or around January 15, 2017, a police officer was dispatched to a residence in West Milton, Ohio. The occupant reported that his son had located an abandoned cellular

telephone on a nearby street. This abandoned cellular telephone was turned over to the officer. The officer thereafter received a telephone call from **HITCHINGS**, who reported that he was the owner of the abandoned telephone. The officer requested that **HITCHINGS** provide proof that he was the owner of the telephone. A few weeks later, an officer released the telephone to **HITCHINGS** (although the report did not detail what proof, if any, that **HITCHINGS** provided that he was the owner of the telephone). **HITCHINGS** signed a property receipt for the telephone. On this receipt, he identified that his telephone number was the TARGET CELL PHONE.

67. Records from the Ohio Bureau of Motor Vehicles identified that **HITCHINGS** utilized the **SUBJECT PREMISES** (the address associated with the TARGET CELL PHONE) on his current Ohio driver's license. Records from the Ohio Bureau of Motor Vehicles also identified that the **SUBJECT VEHICLE** is registered to **HITCHINGS** at the **SUBJECT PREMISES.**

68. Records from the Ohio Bureau of Motor Vehicles identified that three other individuals utilized the **SUBJECT PREMISES** on their current Ohio driver's licenses: SWEENEY, RYAN WESTENDORF (hereinafter referred to as "WESTENDORF"), and ANDREW BAKER (hereinafter referred to as "BAKER"). Records from the Miami County (Ohio) Auditor's website identified that SWEENEY presently owns the **SUBJECT PREMISES.**

Business Records

69. Records from the Ohio Secretary of State identified that SWEENEY registered two business trade names in 2013: Sweeney Communications and Clear Voice One. The registration paperwork identified that the business address for both businesses was the **SUBJECT PREMISES**. The paperwork identified that the general nature of the Sweeney Communications business was "Communications Equipment Sales and Service and Computer Network Sales and Service". The paperwork identified that the general nature of the Clear Voice One business was "VOIP Phone Systems". The trade name for Clear Voice One expired and was cancelled by the Secretary of State in 2018.

70. Records from the Ohio Secretary of State also identified that in 2013, SWEENEY filed Articles of Incorporation for a business with the name of East Main Technologies (the same name as that in the subscriber information received from Charter Communications for the two IP addresses utilized to access the whitchings Facebook account and the w.hitchings@gmail.com Google account). SWEENEY was listed as the statutory agent for this business, and his address was listed as being the **SUBJECT PREMISES.**

71. As part of the investigation, I have accessed various Internet websites that provide information about businesses. One of these websites (www.buzzfile.com) identified that Sweeney Communications, which also does business under the name of Clear Voice One, operates in the local and long distance telephone communications business. Another website (www.zoominfo.com) identified that Clear Voice One provides low cost Voice Over Internet Protocol (VOIP) phone services to businesses and residences.

a. It should be noted that the websites noted above do not always fully verify the information regarding the businesses, nor do they always update records in a timely manner. Therefore, the information noted above may not be current or completely accurate.

72. A website was located for what appeared to be SWEENEY's Clear Voice One business at www.clearvoice1.com. However, this website is not currently operational. A Facebook social media account was located for Clear Voice One, but there were not any public postings to this account since 2017. No websites were located for Sweeney Communications. It therefore appears that these business may no longer be operational.

73. A website was located for East Main Technologies at www.eastmaintech.com. According to this website, the company provides various computer services to businesses and residences, such as network monitoring, cloud backup, peripheral support, anti-virus protection, workstations, and other management of servers. A Facebook account was also located for East Main Technologies.

74. Social media accounts that appear to be utilized by SWEENEY were located on the publicly available information of the Facebook, Instagram, and Twitter websites. Postings were found on these social media accounts indicating that SWEENEY was employed at Walmart. No recent postings were found indicating that SWEENEY worked at or operated East Main Technologies, Clear Voice One, or Sweeney Communications.

75. A social media account that appears to be utilized by WESTENDORF was located on the publicly available information of the Facebook website. The profile page for the account indicated that WESTENDORF was employed in Client/Vendor Relations, Systems Support, and "Dog Mother" for East Main Technologies as well as in Sales, Technical Support, and Graphic Design for Clear Voice One.

76. The whitchings Facebook account was located on the publicly available information of the Facebook website. No information was located on this account indicating that **HITCHINGS** worked at or operated East Main Technologies, Clear Voice One, or Sweeney Communications.

77. As part of the investigation, an FBI Task Force Officer contacted the City of Troy (Ohio) Income Tax Department. A representative from the Income Tax Department provided the following information:

a. The City of Troy Income Tax Department has not received any business income tax returns for Clear Voice One, Sweeney Communications, or East Main Technologies. It should be noted that business tax returns are not required for businesses if they are operated by sole owners. In such cases, the owner is required to report his/her business income on a Schedule C of his/her federal return. The City of Troy Income

Tax Department requests that the Schedule C's be attached to the city returns.

b. The City of Troy Income Tax Department has received personal income tax returns from SWEENEY. His 2019 return identified that he had a business loss of approximately $7,000. However, his Schedule C did not identify the name or type of business that generated this loss. Returns that the City of Troy Income Tax Department received from SWEENEY prior to 2019 did not include any Schedule C forms, indicating that he did not have any business income or losses.

c. The City of Troy Income Tax Department has not received any personal income tax returns for **HITCHINGS** or WESTENDORF in any previous tax years.

78. Based on the information detailed above, some of the computer and electronic media (such as the servers) depicted in the images and videos recovered from the SUBJECT VERIZON CLOUD ACCOUNT could be related to the current or historical operation of the Clear Voice One, Sweeney Communications, and/or East Main Technologies businesses. However, based on the information detailed above, these businesses either do not appear to be currently operational and/or do not appear to be generating any profits or significant income.

79. Based on the following, as well as other information detailed in the Affidavit, **HITCHINGS** appears to be the primary user of the computer and electronic media located in the basement of **SUBJECT PREMISES**:

a. Based on the images and videos recovered from the SUBJECT VERIZON CLOUD ACCOUNT and the o0bc0o Skype account, it appears that **HITCHINGS** regularly uses computer equipment (including the servers) located in the basement of the **SUBJECT PREMISES**.

b. No images were recovered from the SUBJECT VERIZON CLOUD account that depicted SWEENEY using the computer equipment in the basement.

c. As detailed above, the user of the o0bc0o Skype account talked about using his server to operate a website that promotes individuals having a sexual fetish in gear.

d. As detailed above, the user of the o0bc0o Skype account made comments consistent with someone who maintains child pornography files on cloud accounts and/or servers.

e. Again as detailed above, Adult Male A reported that **HITCHINGS** utilized computer media in the basement of the **SUBJECT PREMISES** to show Adult Male A videos depicting child pornography and to download child pornography files onto a computer that was given to Adult Male A.

80. **HITCHINGS** does not appear to have any association with the operation of SWEENEY's

businesses. Based on all of the information detailed in the Affidavit, there is probable cause to believe that the computer and electronic media located in the basement of the **SUBJECT PREMISES** contain evidence of **HITCHINGS'** child pornography activities.

Surveillance Activities

81. An FBI Task Force Officer and I have driven by the **SUBJECT PREMISES** on a number of occasions. During these times, the following was noted:

a. The location of the **SUBJECT PREMISES** is consistent with the description provided by Adult Male A of **HITCHINGS'** residence.

b. The **SUBJECT VEHICLE** has been consistently parked in the driveway of the **SUBJECT PREMISES**, as recently as on or around February 4, 2021.

c. A vehicle registered to SWEENEY has also been parked in the driveway of the **SUBJECT PREMISES** on several occasions, as recently as on or around February 4, 2021. Vehicles registered to BAKER have not been seen at the **SUBJECT PREMISES** on any occasions.

d. There are a number of surveillance cameras attached to the **SUBJECT RESIDENCE** that appear to capture all sides of the residence.

Conclusion Regarding Accounts and Criminal Conduct

82. Based on all of the information detailed in the Affidavit, there is probable cause to believe that **HITCHINGS** resides at the **SUBJECT PREMISES**, is the owner and user of the **SUBJECT VEHICLE**, and is the user of the following:

a. The TARGET CELL PHONE and the SUBJECT VERIZON CLOUD ACCOUNT;

b. The email addresses w.hitchings@gmail.com, hitchingsw@gmail.com, and wenglebot@yahoo.com;

c. The whitchings Facebook account;

d. The o0bc0o Skype account; and

e. The Dropbox account associated with the email address w.hitchings@gmail.com.

83. Also based on all of the information detailed in the Affidavit, there is probable cause to believe that **HITCHINGS** has used computer devices (including the TARGET CELL PHONE and other computer and electronic media located at the **SUBJECT PREMISES**) to possess, receive, and distribute child pornography files. There is also probable cause to

believe that **HITCHINGS** has utilized electronic accounts (including the o0bc0o Skype account) to discuss the sexual exploitation of children and his child pornography activities

84. Again based on all of the information detailed in the Affidavit, there is probable cause to believe that **HITCHINGS** has possessed controlled substances. As detailed above, images and videos recovered from the SUBJECT VERIZON CLOUD ACCOUNT indicate that **HITCHINGS** has possessed controlled substances in the basement of the **SUBJECT PREMISES**. Based on my training and experience, the drug paraphernalia depicted in some of these images and videos (such as the scales and packaging materials) as well as the quantities and weights of some of the substances depicted in the images and videos are consistent with someone who distributes controlled substances. **HITCHINGS'** communications recovered from the o0bc0o Skype account about having a "runner" and sharing controlled substances with his associates is again consistent with someone who distributes controlled substances.

85. Based on the following information, as well as other information detailed in the Affidavit, there is probable cause to believe that **HITCHINGS** has possessed firearms as a prohibited person, and that one or more firearms may be located at the **SUBJECT PREMISES**, on his person, and/or the **SUBJECT VEHICLE**:

a. As detailed above, **HITCHINGS** was arrested in Florida in 2010 after he was found in possession of a handgun, ammunition, cocaine, and drug paraphernalia in his vehicle. He subsequently pled guilty to Felony Possession of Cocaine

b. Images recovered from the SUBJECT VERIZON CLOUD ACCOUNT indicate that **HITCHINGS** took photographs of himself possessing a handgun in 2016 (when he was prohibited from possessing firearms based on his prior conviction).

c. A video file recovered from the Dropbox account associated with the w.hitchings@gmail.com account indicates that **HITCHINGS** took multiple photographs of himself possessing a handgun in or around 2017 (when he was prohibited from possessing firearms based on his prior conviction).

d. The contents of the o0bc0o Skype account include communications where **HITCHINGS** identified that he was carrying a 9-millimeter handgun. During these communications, **HITCHINGS** expressed thoughts of using this handgun to harm himself and thoughts of using firearms to harm police officers.

e. Based on my training and experience, I know that individuals involved in drug trafficking offenses frequently maintain firearms and weapons to protect their controlled substances and the proceeds derived from their sales.

f. As detailed above, the investigation has identified that **HITCHINGS** has surveillance cameras on the interior and exterior of his residence. **HITCHINGS** also indicated in his communications via the o0bc0o Skype account that he utilized

security practices to protect himself from criminal culpability for his child pornography activities. All of these communications are consistent with individuals who use firearms to protect their controlled substances, the proceeds derived from their drug sales, and/or the contraband from other criminal activities (to include child pornography offenses).

Evidence Sought in Search Warrants for Child Pornography Offenses

86. Based on my training and experience, I know that it is not uncommon for individuals involved in child pornography offenses to utilize multiple computer devices in furtherance of their child pornography and child exploitation activities. Individuals sometimes save their files to multiple devices to allow easy access to the files and/or to back-up the devices in case of a computer failure.

87. Again based on my training and experience, I know that collectors of child pornography often use external devices (such as thumb drives, external hard drives, CD's/DVD's, SD cards, SIM cards, etc.) to store child pornography. The accumulation of child pornography files may fill up the space on the hard drives of computers, and external devices are needed to store and maintain files. These devices also serve as a mechanism for transferring files from one computer to another. In my experience, individuals maintain such external devices in their residences. Given their portable size, individuals sometimes maintain the devices on their persons and/or take the devices with them when they travel by vehicle.

88. Based on my training and experience, I know that individuals are increasingly utilizing laptop computers and other smaller devices such as cellular telephones, iPads, and tablets to do their computing. These devices are typically maintained in the owners' residences. Due to their portable nature, individuals also sometimes maintain the devices on their persons and/or take the devices with them when they travel by vehicle.

89. Based on my training and experience, I know that collectors of child pornography often maintain their collections for long periods of time. In addition, computer evidence typically persists for long periods of time, and computer data can often be recovered from deleted space (as further detailed above).

90. Based on my training and experience, individuals involved in child exploitation schemes often utilize social media accounts, email addresses, messenger applications, and dating websites as a means to locate and recruit victims. They then use the chat functions on these websites, as well as email accounts and other messenger applications, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

91. Also based on my training and experience, I know that individuals involved in child exploitation offenses utilize a variety of threats and manipulation techniques to compel their victims to engage or continue engaging in the illicit sexual activities (including the

production of child pornography). These threats and manipulations are intended to control the victims and their activities, prevent them from stopping the activities, and prevent them from contacting law enforcement officers. It is common for such offenders to threaten that if the victims end the illicit sexual activities, the offenders will harm the victims and their family members and / or bring notoriety and shame to the victims by exposing the victims' involvement in the sexually explicit conduct.

92. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses via e-mail, social media, and other online chatrooms. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

93. In my experience, individuals often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, and on Internet bulletin boards; Internet P2P file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email communications. Evidence of the multiple aliases, accounts, and sources of child pornography are often found on the computer devices located at the offenders' residences, in their vehicles, and on their persons.

94. I know, in my experience, that individuals involved in child exploitation offenses sometimes print the pictures in hard copy format. Such individuals do so both for easier access / viewing of the files and to back-up the files in the event that one computer device becomes damaged and broken. Similarly, these individuals often save contact information (i.e., email addresses and account names) for those with whom they communicate about child exploitation offenses in multiple locations.

95. In addition, individuals often maintain lists of their electronic accounts (including associated user names and passwords) and their aliases in handwritten format. These papers are sometimes maintained in close proximity to their computers for easy access. In other cases, the papers may be hidden or maintained in secure locations to avoid detection by others.

96. As detailed above, there are at least three businesses that purportedly have operated out of the **SUBJECT PREMISES**. Based on my training and experience, I know that individuals who operate businesses out of their homes typically keep business records in their homes. I also know, based on my training and experience, that individuals who conduct criminal activities in their homes sometimes utilize businesses as a "front" to conceal their activities. Therefore, any business records located at the **SUBJECT PREMISES** are materially relevant to the investigation in that they would help to determine whether or not the businesses are legitimate. If it is determined that the businesses are legitimate, these records would still be materially relevant to the investigation in that they would help to determine which computer devices are utilized by **HITCHINGS** and which devices relate to the

businesses. Making such a determination would be essential in determining who is responsible for any contraband contained on the Computer and Electronic Media seized pursuant to the proposed search warrants.

97. As detailed above, there appears to be surveillance cameras that capture the interior and exterior of the **SUBJECT PREMISES**. This surveillance footage could be materially relevant in that it could provide evidence of who was inside the residence at the times the child pornography activities and/or drug offenses were committed. Furthermore, depending on the locations of the cameras inside of the residence, this surveillance footage could capture **HITCHINGS** and his co-conspirators conducting the child pornography and drug activities.

98. In my experience, I know that many cellular telephones, iPads, and tablets store information related to IP addresses and Wi-Fi accounts that the telephone accessed and GPS data. This information helps in identifying the subjects' whereabouts during the criminal activities and the travels they took to get to these locations.

Evidence Sought in Search Warrants for Drug Offenses

99. Based on my training and experience, and in discussions with other law enforcement officers, I have learned the following:

a. Individuals involved in possessing and using controlled substances often maintain controlled substances, drug paraphernalia, and documents related to their drug activities in their residences, on their persons, and in their vehicles. Drug paraphernalia may include scales used to weigh the controlled substances, items used to package controlled substances (such as baggies, balloons, and capsules), items used to consume controlled substances (such as pipes, bongs, needles, mirrors, razor blades, straws, spoons, hypodermic needles, and cigarette papers), and items used to dilute or alter controlled substances (such as baking soda, hydrochloride, mannitol, mannite, dextrose, or lactose).

b. Individuals involved in distributing controlled substances frequently maintain at their residences, places of business, or other secure premises to which they have access, amounts of controlled substances and amounts of currency in order to maintain and finance their ongoing business.

c. Narcotics traffickers frequently maintain various records (such as books, records, receipts, notes, ledgers, airline tickets, money orders, and other papers) related to the transportation, ordering, sale, and distribution of controlled substances. Furthermore, I know that the aforementioned books, records, receipts, notes, ledgers, etc. are generally maintained where the traffickers have ready access to them.

d. Narcotics traffickers use and maintain electronic devices in furtherance of their illegal activities (to include but not limited to cellular telephones, computers, paging devices, answering machines, police scanners, and money counters) and to facilitate their criminal activity.

e. It is common for drug traffickers to secure contraband, proceeds of drug sales, and records of drug transactions in secure locations within their residences or places of business as a means of concealing the same from law enforcement authorities.

f. Persons involved in drug trafficking activities often conceal proceeds of drug sales, records of drug transactions, firearms, ammunition, caches of drugs, large amounts of currency, financial instruments, keys to safe deposit boxes, precious metals, jewelry, other items of value, and/or evidence of financial transactions utilized in furtherance of narcotics trafficking in their residences and in other secure locations including places of business in order to conceal them from law enforcement authorities.

g. Narcotics traffickers commonly maintain records of telephone calls in billing statements, as well as addresses or telephone numbers in books or papers which reflect names, addresses, and telephone numbers of their co-conspirators.

h. Individuals involved in drug offenses often take photographs and video recordings of their controlled substances and drug paraphernalia (such as the images and videos detailed above that were recovered from the SUBJECT CLOUD ACCOUNT and the o0bc0o Skype account).

i. Narcotics traffickers utilize vehicles to transport and conceal narcotics.

j. Narcotics traffickers frequently maintain firearms and weapons to protect both the controlled substances and proceeds derived from their sales. Narcotics traffickers maintain firearms as a use of force, or threat of force, against rival drug dealers and/or delinquent customers.

Evidence Sought in Search Warrants for Drug Offenses

100. Based on my training and experience, I know that individuals involved in firearms offenses typically maintain firearms and ammunition at their residences, on their persons, and in their vehicles. I also know, based on my training and experience, that individuals often keep the boxes, holsters, extra magazines, and other accessories to the firearms they purchase in their residences, on their persons, and in their vehicles.

101. Based on my training and experience, I know that individuals often tender and obtain various documents when they purchase firearms. These documents may include the sales receipts, bills of sale, owners' manuals, and other similar documents. Such documents are often maintained in the owners' residences and vehicles and on their person.

102. Based on the investigation, it appears that **HITCHINGS** resides at the **SUBJECT PREMISES** with SWEENEY and WESTENDORF. SWEENEY and WESTENDORF have not been convicted of any prior felony offenses, and as such, are not prohibited from possessing firearms. Authority is therefore requested to search for and seize any firearms and associated items to which is appears that **HITCHINGS** has reasonable access to in the **SUBJECT PREMISES** and in the **SUBJECT VEHICLE.**

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

103. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

104. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

105. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

106. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. On-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. Examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. Surveying various file directories and the individual files they contain;

f. Opening files in order to determine their contents;

g. Scanning storage areas;

h. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachments B-1 through B-3; and

i. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachments B-1 through B-3.

107. Based on the photographs, video recordings, and communications recovered from **HITCHINGS'** accounts (as detailed above), it appears that there are Computer and Electronic Media containing a significant amount of storage space at the **SUBJECT PREMISES** (potentially in excess of 100 TB). Based on communications recovered from **HITCHINGS'** accounts related to his security practices and the document contained in **HITCHINGS'** Dropbox account related to a BitLocker recovery key (as detailed above), it is reasonable to believe that these devices may contain encryption.

108. Based on my training and experience and in consultation with FBI computer examiners, I know that most if not all encryption software typically makes the contents of the encrypted devices or containers extraordinarily difficult, if not effectively impossible, to access if the owner/user of such devices does not provide the necessary passwords. However, if the Computer and Electronic Media containing such encryption are located by law enforcement officers in a powered on state, the contents may be unencrypted and accessible. Powering off such devices or otherwise interrupting the power supply in any way would result in the contents being encrypted and inaccessible in a laboratory setting. As such, the only effective way for law enforcement officers to access the contents of encrypted containers is to image the devices on-scene before the power source is interrupted.

109. Also based on my consultation with FBI computer examiners, I know that imaging servers is typically best and most accurately completed while they are intact and powered on. Depending on the type and construction of the server, attempting to disassemble it and properly reassemble it in another environment could risk loss of evidence.

110. Based on consultation with FBI computer examiners, imaging what could be over 100 TB of data will take a significant period of time. The examiners are unable to provide an estimate of the amount of time that may be needed to image the Computer and Electronic Media at the **SUBJECT PREMISES** without assessing the servers and other devices, without knowing the specific hardware of the devices, and without knowing how many devices are powered on and encrypted. However, if a significant number of the computer devices are powered on and encrypted, and if the residents at the **SUBJECT PREMISES** do not cooperate in providing the passwords, imaging the devices could take multiple days. Authority is therefore requested to remain at the **SUBJECT PREMISES** until any necessary imaging the devices can be completed, including during overnight hours.

CONCLUSION

111. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located at the **SUBJECT PREMISES**, the person of

ATTACHMENT A-1

DESCRIPTION OF LOCATION TO BE SEARCHED

924 EAST MAIN STREET, TROY, OHIO, 45373 ("SUBJECT PREMISES"), is a two-story, single-family residence with white siding. There is a front porch with white pillars leading to the front door. The street address numbers are affixed to the siding next to the front porch. There is a detached one-car garage with white siding and a white overhead door. The SUBJECT PREMISES is located on the north side of East Main Street between East Franklin Street and Williams Street. The SUBJECT PREMISES includes all outbuildings, curtilage, and vehicles parked on the property of the SUBJECT PREMISES.

The warrant authorizes law enforcement officers to remain at the SUBJECT PREMISES during the overnight hours if the search (to include the imaging of any Computer and Electronic Media) cannot be completed prior to 10:00 p.m.

ATTACHMENT B-1

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography), 18 U.S.C. § 922(g) (possession of a firearm by a prohibited person), 21 U.S.C. § 844 (possession of controlled substances), and 21 U.S.C. § 844 (distribution or possession with intent to distribute controlled substances), including but not limited to the following:

Computers and Electronic Media

1. The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with the affidavit submitted in support of this warrant.

2. Computer hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks); cellular telephones and tablets; and digital cameras and recording devices.

3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents, and materials referencing or relating to the above-described offenses. Such records, documents, or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data obtained through computer or Internet-based communications, including data in the form of electronic records, documents, and materials, including those used to facilitate interstate communications, including but not limited to telephone (including mobile telephone), tablets, and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer- related equipment, such as fixed disks, external

hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records and Physical Records

9. Any records related to the possession, receipt, and distribution of child pornography.

10. Any images or videos depicting child pornography.

11. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

12. Any Internet history indicative of searching for child pornography.

13. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.

14. Any communications with minors.

15. Evidence of utilization of email accounts, messenger applications, social media accounts, online chat programs, and peer-to-peer file sharing programs.

16. Any information related to Internet Protocol (IP) addresses accessed by the computer and electronic media.

17. Any Wi-Fi and GPS data associated with the computer and electronic media.

18. Lists of computer and Internet accounts, including user names and passwords.

19. Any computer passwords and encryption keys.

20. Any information related to the use of aliases.

21. Any records, documents, and billing records pertaining to accounts held with telephone, electronic, and Internet service providers.

22. Any and all diaries, notebooks, notes, and other records reflecting personal contact and any other activities with minors.

23. Any children's clothing, toys, or other belongings.

24. Quantities of controlled substances.

25. Any drug paraphernalia, including but not limited to scales used to weigh the controlled substances, items used to package controlled substances (such as baggies, balloons, and

capsules), items used to consume controlled substances (such as pipes, bongs, needles, mirrors, razor blades, straws, spoons, hypodermic needles, and cigarette papers), and items used to dilute or alter controlled substances (such as baking soda, hydrochloride, mannitol, mannite, dextrose, or lactose).

26. Any communications regarding the purchase or sale of controlled substances.

27. Log books, records, payment receipts, notes, and/or customer lists, ledgers, and other papers or electronic records related to the transportation, ordering, purchasing, processing, and distribution of controlled substances.

28. Papers, tickets, notices, credit card receipts, travel schedules, travel receipts, passports, and/or records or other items related to domestic and foreign travel to obtain and distribute controlled substances and drug proceeds, including but not limited to airline receipts, vehicle rental receipts, credit card receipts, travel schedules, diaries, hotel receipts, truck logs, travel agency vouchers, notes, records of long distance telephone calls, emails, and other correspondence.

29. Address and/or telephone books and papers reflecting names, email and physical addresses, and/or telephone numbers of individuals, partnerships, or corporations involved in drug trafficking.

30. Financial records, financial statements, receipts, statements of accounts and related bank records, drafts, letters of credit, money orders, cashier's checks, passbooks, bank checks, escrow documents, and other items evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, secreting, transferring, concealment, and/or expenditure of money.

31. Any surveillance related equipment and any surveillance footage depicting the SUBJECT PREMISES and/or William Sidney Hitchings V.

32. United States currency, precious metals, coins bullion, jewelry, and financial instruments.

33. Photographs and video recordings of controlled substances and drug paraphernalia.

34. Any firearms and ammunition of which WILLIAM SIDNEY HITCHINGS V may reasonably have access to at the SUBJECT PREMISES.

35. Documents and communications related to the purchase and acquisition of firearms and ammunition;

36. Gun boxes, gun holsters, magazines, and other firearm accessories

37. Any records, documents, and billing records pertaining to accounts held with telephone, electronic, and Internet service providers.

38. Any business records related to the operation of Sweeney Communications, Clear Voice One, East Main Technologies, or any other businesses operating at the SUBJECT PREMISES or by WILLIAM SIDNEY HITCHINGS V.

39. Records of personal and business activities relating to the operation and ownership of the computer and electronic media seized from the SUBJECT PREMISES.

40. Documents and records regarding the ownership and/or possession of the items seized from the SUBJECT PREMISES.

Photographs of Search

41. During the course of the search, photographs of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items seized from the residence.

HITCHINGS, the **SUBJECT VEHICLE**, and the Computer and Electronic Media (as defined in Attachments B-1 through B-3) located at the **SUBJECT PREMISES**, on the person of **HITCHINGS**, and in the **SUBJECT VEHICLE**, and the Computer and Electronic Media (as defined in Attachments B-1 through B-3) located at the **SUBJECT PREMISES**, the person of **HITCHINGS**, the **SUBJECT VEHICLE**, and the Computer and Electronic Media (as defined in Attachments B-1 through B-3) located at the **SUBJECT PREMISES**, on the person of **HITCHINGS**, and in the **SUBJECT VEHICLE**: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(1), 18 U.S.C. §§ 2252(a)(2) and (b)(1), 18 U.S.C. §§ 2252A(a)(2) and (b)(1), 18 U.S.C. § 922(g), 21 U.S.C. § U.S.C. § 844, and 21 U.S.C. § 841.

112. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-3.

Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
Before me this 5 of February 2021

CHELSEY M. VASCURA
UNITED STATES MAGISTRATE JUDGE